REMARKS

The basis for the new claims is found at least in the following paragraphs: 0099, 0110, 0115-0120, 0124-0129, 0135, 0137, 0138, 0141, 0144, 0147, and 0150-0153. The amendments to claims 48, 53, 66, 72, 76 and 77 are editorial in nature and do not narrow the scope of the inventions defined therein. Favorable consideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

Respectfully submitted,

Date September 24, 2001

By _____

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

Please amend the specification as follows:

Page 15, paragraph 56:

In a further aspect, the present invention comprises the steps of: generating said counter anew for every new key; initializing generated counter to a constant value; for each message being signed using key, incrementing said counter by [the] one; and outputting said counter as an output block of the authentication scheme.

Page 16, paragraph 61:

In a further aspect, the present invention comprises the steps of: creating a secret random vector block of ℓ bits in length; performing the same randomization function as that used at a signing method for determining an authentication tag over the plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length; wherein performing the randomization function further comprises: deriving a random initial vector from the string presented for [decryption] verification; generating a sequence of unpredictable elements each of ℓ-bit length from the random initial vector in the same manner as used at signing method; and selecting n plaintext blocks from the string in the same order as that used at the signing method, and combining the selected plaintext blocks and the random vector with a different corresponding element of the sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

In the Claims:

48. (Amended) The method of claim 38, comprising:

generating said counter anew for every new key;

initializing generated counter to a constant value; and

for each message being signed using key, incrementing said counter by [the] one; and

outputting said counter as an output block of the authentication scheme.

53. (Amended) The method as defined in claim 52, further comprising the steps of:

creating a secret random vector block of ℓ bits in length;

performing the same randomization function as that used at a signing method for determining an authentication tag over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein performing said randomization function further comprises:

deriving a random initial vector from said string presented for [decryption] verification;

generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and

selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

66. (Amended) The system as defined in claim 65, further comprising:

a third component for creating a secret random vector block of ℓ bits in length;

wherein the first component performs the same randomization function as that used at the signing method over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein the first component performing said randomization function further comprises:

a component for deriving a random initial vector from said string presented for [decryption] verification;

a component for generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and

a component for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

72. (Amended) The program product of claim [68] 71, wherein the third code for applying the pseudo-random function applies a pseudo-random function that is a standard block cipher.

76. (Amended) The program product as defined in claim [72] 75, further comprising:

seventh code for creating a secret random vector block of ℓ bits in length;

wherein the third code performs the same randomization function as that used at the signing method over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein the third code performing said randomization function further comprises:

code for deriving a random initial vector from said string presented for [decryption] verification;

code for generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and

code for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

77. (Amended) The program product as defined in claim [72] 75, wherein the third code for performing said randomization function further comprises:

code for using a secret, random initial vector shared between sender and receiver;

code for generating a sequence of unpredictable elements each of ℓ-bit length from said secret random initial vector in the same manner as used at signing method; and

code for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.